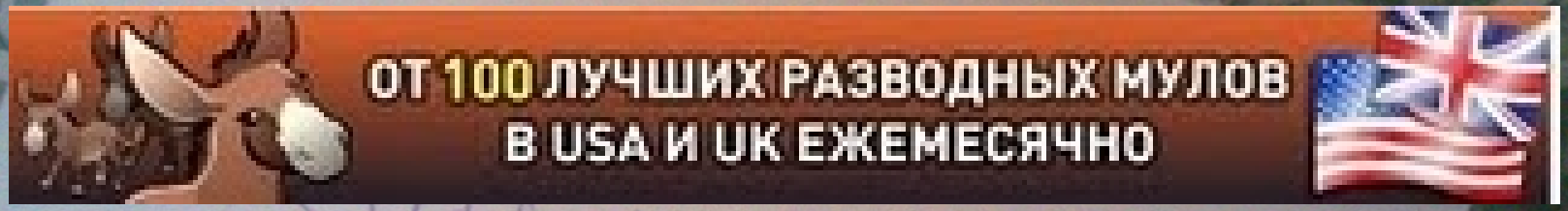
Exposing the Dynamic Money Mule Recruitment Ecosystem



Who is Dancho Danchev?

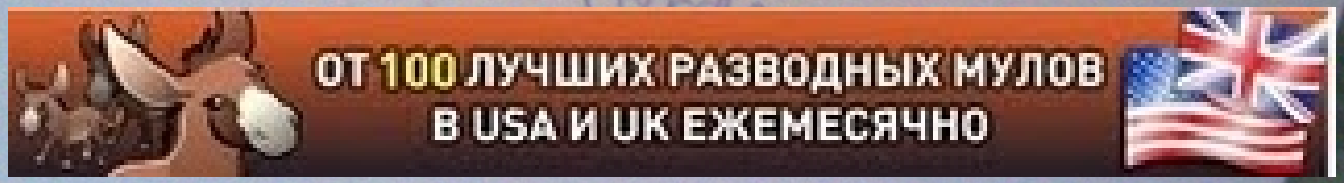
- Independent cyber crime/cyber threats analyst working under non-disclosure agreements – http://ddanchev.blogspot.com
- Security Blogger at CBS Interactive's ZDNet.com – http://blogs.zdnet.com/security

Outline of the Presentation

- Basics of Mule Recruitment
- Current trends within the ecosystem
- What's it like to be a Money Mule?
- Profiling a key vendor of standardized recruitment templates
- When the recruiters go malicious
- Who's providing the DNS infrastructure?
- Who launched the DDoS attack against bobbear.co.uk in 2008?
- Responses to mule recruitment

Basics of Mule Recruitment

- Mule recruitment offers “risk forwarding” to unaware accomplices
- First profiling of recruitment in 2008
  - ASPRox botnet offering fast-fluxed hosting for mule recruitment sites
  - Sophisticated mule recruitment syndicate operating since 2002



Basics of Mule Recruitment

- Requirements to join the group
  - Have been in “business” for at least 6 months
  - At least one recommendation from two cybercrime-friendly communities
  - 45% commission with $3k as minimum payment
  - The partner is required to pay a membership fee in order to continue receiving fraudulently obtained payments
  - The gang’s pitch “From a 100 personal mules from the U.K and the U.S on a monthly basis”

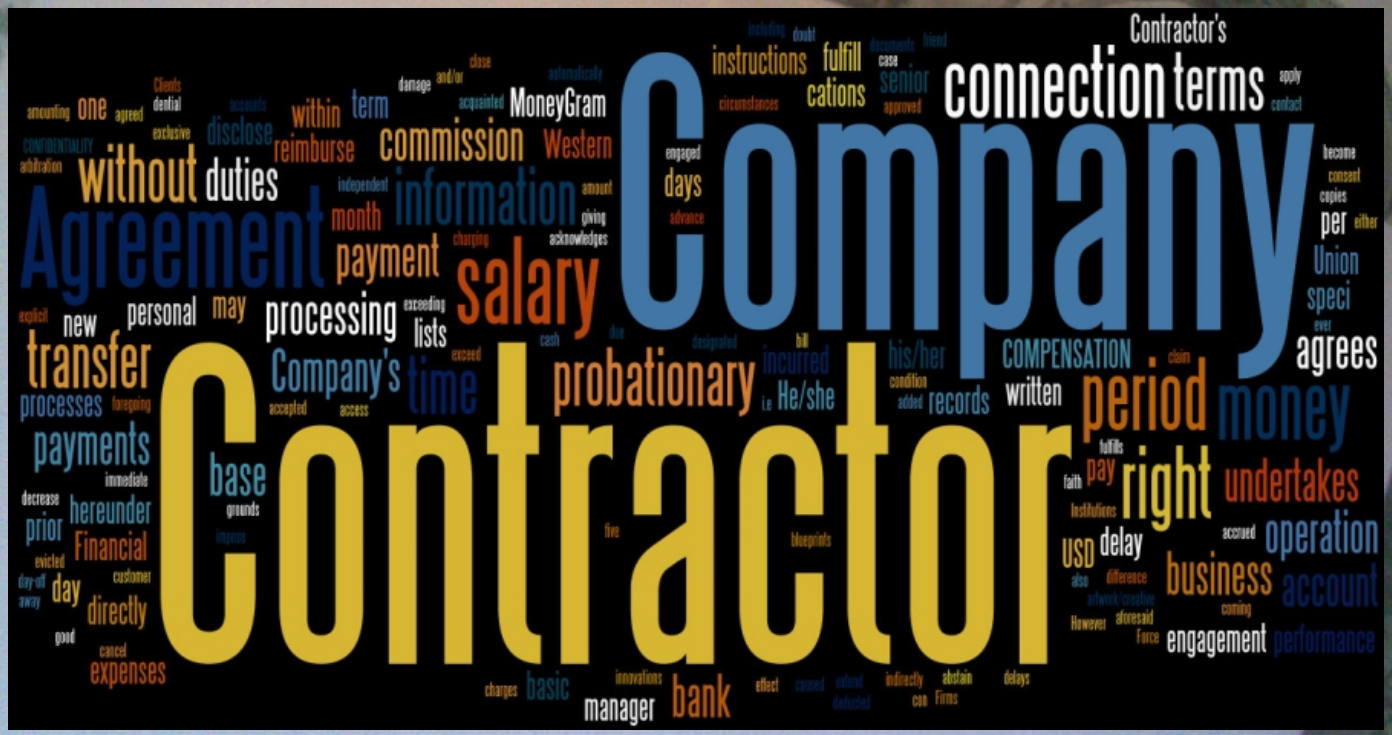
Basics of Mule Recruitment

- The mule recruitment process
  - Stage 01 - Personalization of emails obtained from harvested job postings or segmented spam databases – sometimes come as bonus
  - Stage 02 – Spamvertising.
  - Sample email:

  - The pay is $2,300 per month during the Trial Period + 8% commission from each successfully handled payment. Total income is about $4,500 per month. After the first 30 days your base salary will be increased up to $3,000 a month.

Current trends within the ecosystem

- Stage 03 – Verification of the mule over phone
- Stage 04 – Signing a professionally looking contract, and providing access to user friendly Web-interface



Current trends within the ecosystem

What's it like to be a Money Mule?

Why are you gathering so much information about applicants? Such attention especially to bank account details puts me on guard.

In fact that modern financial system is a complex instrument, which controls financial streams. The problem is that any transfer may be delayed (from 1 to 5 days) but it is unacceptable for our business. Transaction should be completed by a financial manager the same day money is deposited into the bank account. Otherwise, we risk to lose money, clients, reputation. Analyzing all the details below we'll be able to prepare tasks for every agent individually. Please fill in all the fields carefully to avoid delays while working with your bank. The success of our cooperation depends on the accuracy of entered details! Please be serious.

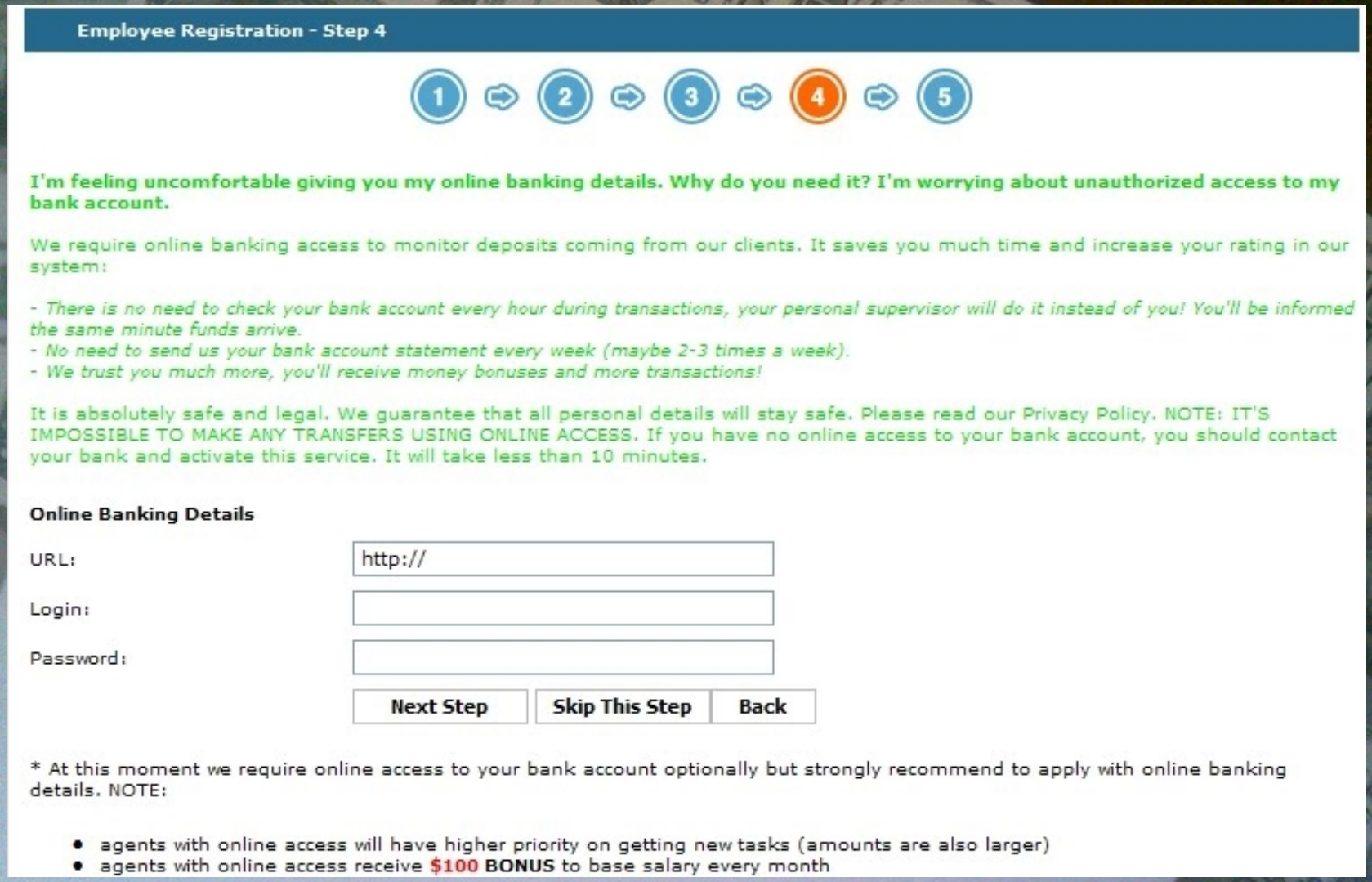
**You are responsible for reliability of this information. If you're having any difficulties please contact your bank.*

Banking Details

Account Type*:	Personal	
Bank Name*:		
Account Type (checking/saving)*:	- select -	
Name on the Account*:		?
Account Number*:		?
Routing Number for ACH transfer*:		?
Routing Number for Federal Wire Transfer*:		?
Date you opened your bank account*:		?
How often do you use your bank account?*:		?
Average amount of each operation*:		
Is it a prepaid account?*:		?
Daily withdrawal limit over the counter*:		?
Have you ever used Western Union/Money Gram?*:		
Are there Money Gram offices in your area?*:		?

Next Step Back

What's it like to be a Money Mule?



Employee Registration - Step 4

1 → 2 → 3 → 4 → 5

I'm feeling uncomfortable giving you my online banking details. Why do you need it? I'm worrying about unauthorized access to my bank account.

We require online banking access to monitor deposits coming from our clients. It saves you much time and increase your rating in our system:

- There is no need to check your bank account every hour during transactions, your personal supervisor will do it instead of you! You'll be informed the same minute funds arrive.
- No need to send us your bank account statement every week (maybe 2-3 times a week).
- We trust you much more, you'll receive money bonuses and more transactions!

It is absolutely safe and legal. We guarantee that all personal details will stay safe. Please read our Privacy Policy. NOTE: IT'S IMPOSSIBLE TO MAKE ANY TRANSFERS USING ONLINE ACCESS. If you have no online access to your bank account, you should contact your bank and activate this service. It will take less than 10 minutes.

Online Banking Details

URL: http://

Login:

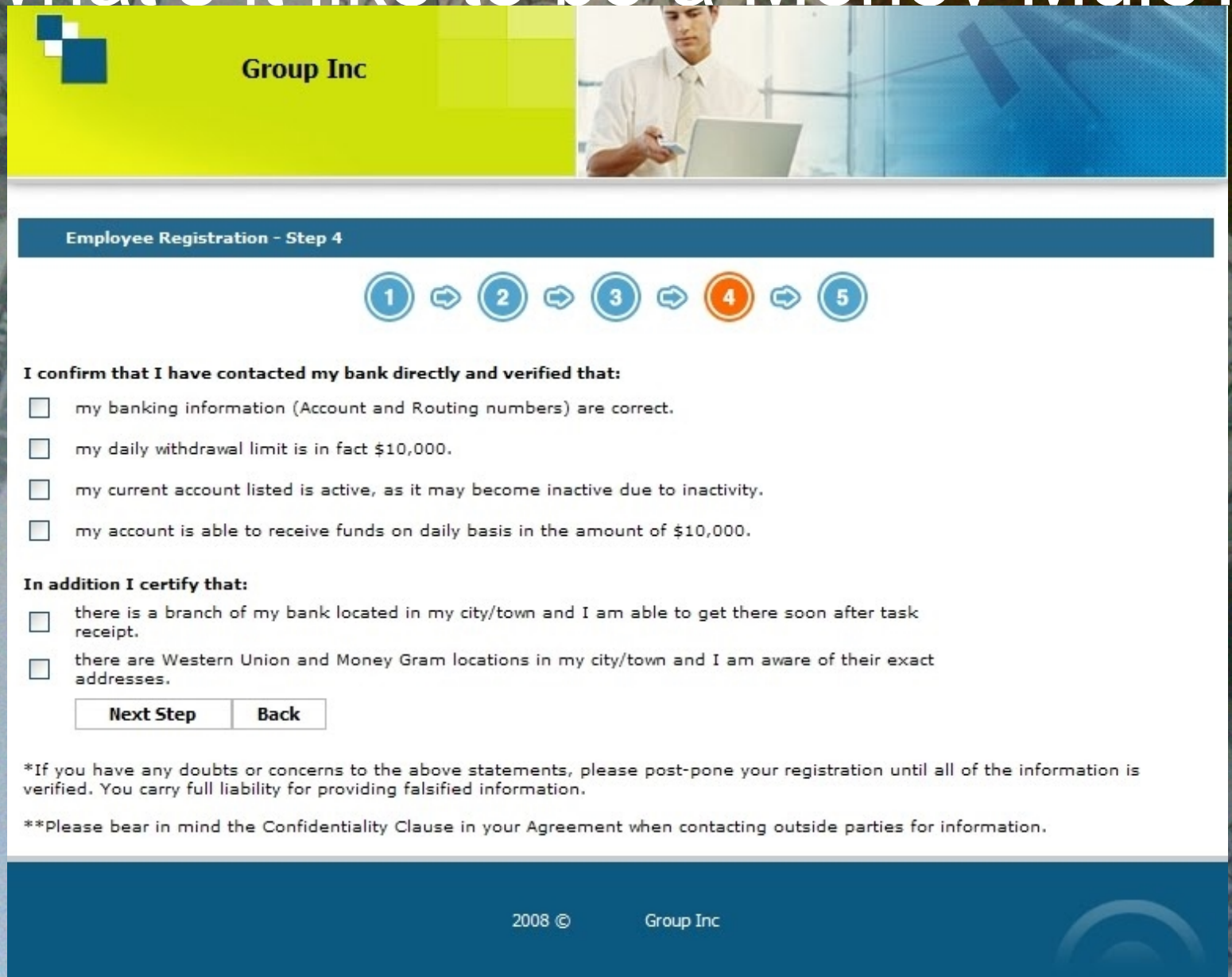
Password:

Next Step | Skip This Step | Back

* At this moment we require online access to your bank account optionally but strongly recommend to apply with online banking details. NOTE:

- agents with online access will have higher priority on getting new tasks (amounts are also larger)
- agents with online access receive **$100 BONUS** to base salary every month

What's it like to be a Money Mule?



Profiling a key vendor of standardized recruitment templates

- Tran$later – key vendor of standardized templates, recruitment documents

Profiling a key vendor of standardized recruitment templates

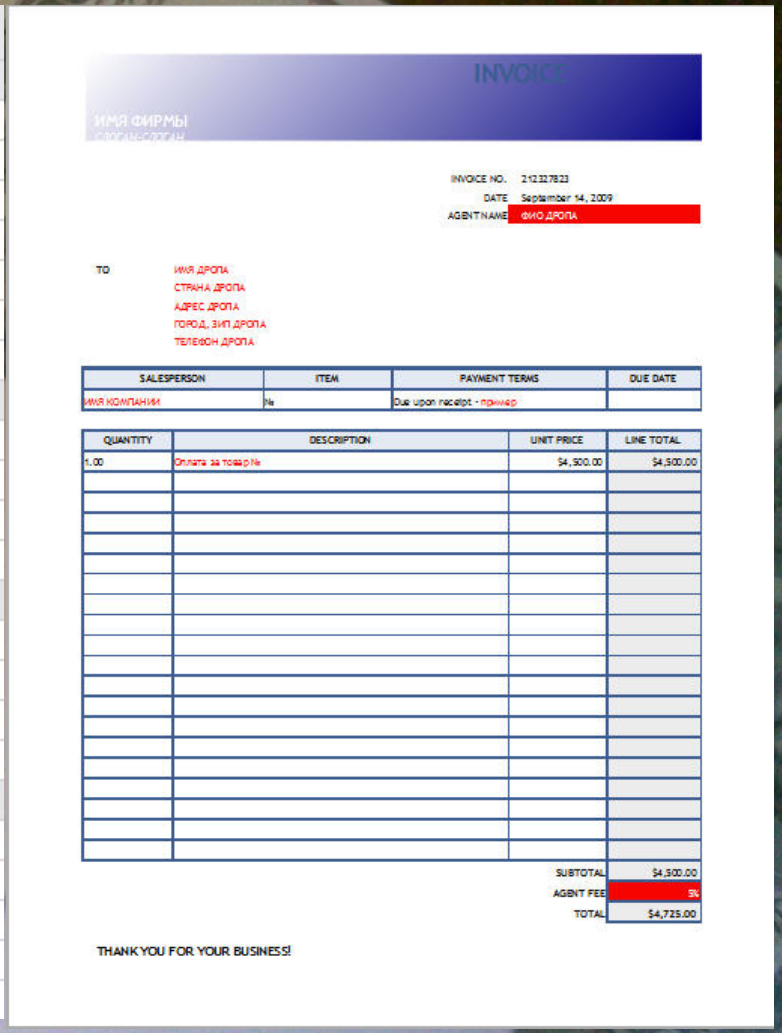
- Personal - 900$
  - Web-site in English
  - Correspondence from the first answer till the output (WU/WIRE/SPLIT)
  - All the covering documentation (contracts, agreements, applications, letterheads, forms etc)
  - Signature, logo, stamp (GIF/PSD)
  - A detailed project manual with advices and recommendations (ENG/RUS)
  - Subsidiary texts for work
  - Spam-letters (HTML or TEXT)

Profiling a key vendor of standardized recruitment templates

- Business - 1700$
  - Corporate site in two languages
  - From A to Z correspondence
  - Full volume documentation (real documents adopted for you)
  - 3 signatures (manager 2x, president 1x)
  - Subsidiary texts and requests
  - Spam-letters (2x) (HTML & TEXT)
  - Domain, hosting (regular one), corporative (domain) e-mail
  - Answering machine with already typed message (from company name) and premium pack Skype (1 month)

Profiling a key vendor of standardized recruitment templates

Наименование	Цена
Бланки, формы, таблицы	
Application form (ENG)	$25.00
Application form electron. (ENG)	$20.00
Application form short (ENG)	$20.00
Сопроводительная форма для отправления MG (ENG) (ONE)	$20.00
Сопроводительная форма для отправления MG (ENG) (SPLIT)	$20.00
Сопроводительная форма для отправления WU (ENG) (ONE)	$20.00
Сопроводительная форма для отправления WU (ENG) (SPLIT)	$25.00
Espanol	
Formulario de Inscripcion (ESP) (.DOC)	$35.00
Сопроводительная форма для отправления WU (ESP) (SPLIT)	$30.00
Форма для банковских деталей (ESP) (EEUU)	$25.00
Форма для отправленного перевода WU (ESP)	$20.00
Italian	
Application form (ITAL)	$30.00
Сопроводительная форма для отправления WU (ITAL)	$20.00
Форма для банковских деталей (ITAL) (EU)	$25.00
Форма для отправленного перевода WU (ITAL)	$25.00
Формы для банковских деталей	
Bank Details Form /IBAN/ (ENG)	$25.00
Bank Details Form /AU/ (ENG)	$25.00
Bank Details Form /CA/ (ENG)	$25.00
Bank Details Form /UK/ (ENG)	$25.00
Bank Details Form /US/ (ENG)	$25.00



INVOICE

ИМЯ ФИРМЫ

INVOICE NO. 2123237823
DATE September 14, 2009
AGENT NAME ФИО ДРОПА

TO
ИМЯ ДРОПА
СТРАНА ДРОПА
АДРЕС ДРОПА
ГОРОД, ЗИП ДРОПА
ТЕЛЕФОН ДРОПА

SALESPERSON	ITEM	PAYMENT TERMS	DUE DATE
ИМЯ КОМПАНИИ	№	Due upon receipt - пример	

QUANTITY	DESCRIPTION	UNIT PRICE	LINE TOTAL
1.00	Оплата за товар №	$4,500.00	$4,500.00

SUBTOTAL $4,500.00
AGENT FEE 5%
TOTAL $4,725.00

THANK YOU FOR YOUR BUSINESS!

When the recruiters go malicious

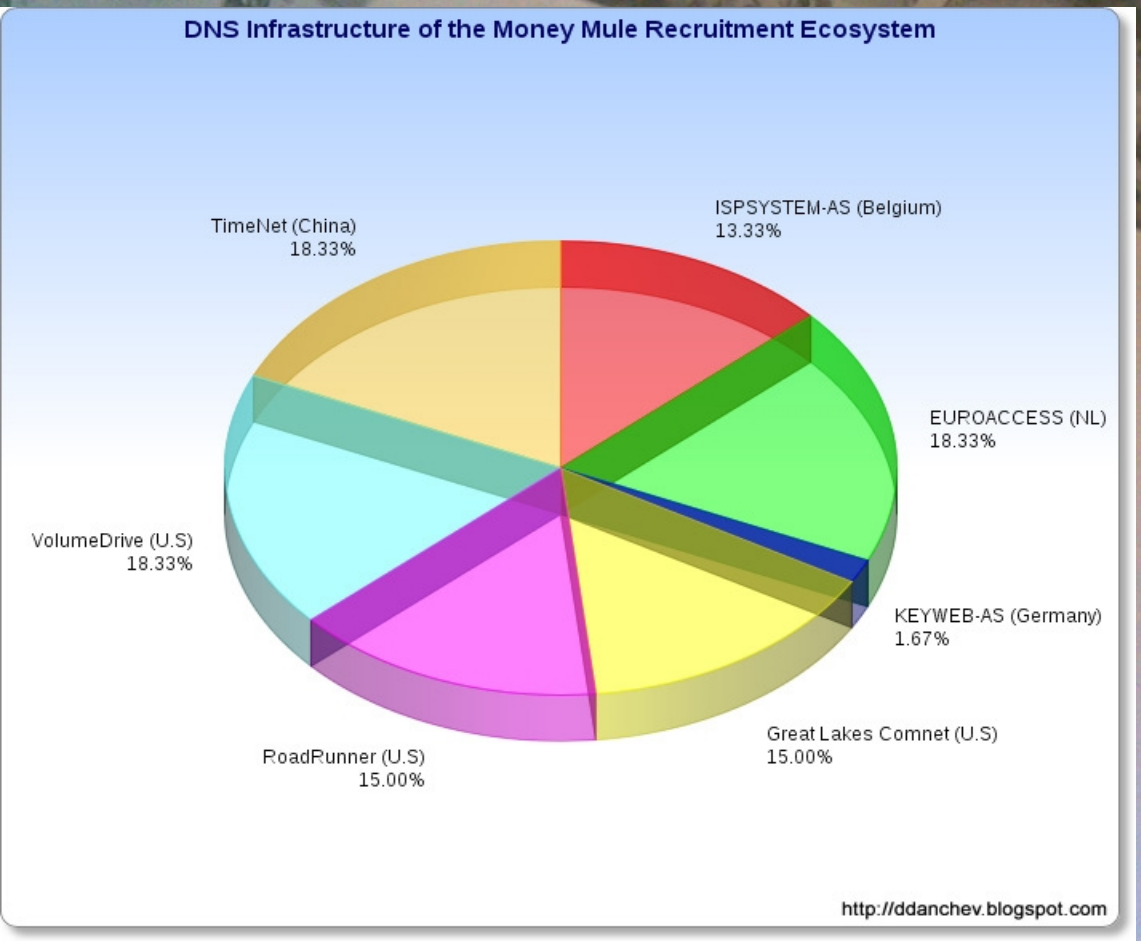
- Undermining OPSEC by infecting the researcher/LE officer with malicious code
- March, 2010, targeted email received from Cefin Consulting & Finance, email account wasn't a spam trap, recruitment site was serving client-side exploits
- The irony? An unsecured directory offered a peek at the spam-as-a-service hosted there

When the recruiters go malicious

- Sprott Asset Management is offering an executable SSL Certificate, which blocks access to sites profiling money mule recruitment campaigns.

Who's providing the DNS infrastructure?

- Every country has it's own share, based on an experiment with active domains



Cybercrime should stop being treated as a country/region specific problem, instead it should be treated as an international problem, with each and every country having its own share of cybercrime activity.

Who launched the DDoS attack against bobbear.co.uk in 2008?

- The same Russian DDoS for hire service, that was also used in the Russia vs Georgia cyber attacks.
- Has been in operation for 5+ years
- So successful that it's using a franchise model => novice cybercriminals rebrand the same service and promote it around cybercrime-friedly forums

Who launched the DDoS attack against bobbear.co.uk in 2008?

Black Energy botnet status at 01:27:33 18.11.2008:

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 1
attack_mode = 0
max_sessions = 30
http_freq = 100
http_threads = 3
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 50
http_threads = 4
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http bobbear.co.uk
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 50
http_threads = 4
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http bobbear.co.uk
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 50
http_threads = 4
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http bobbear.co.uk
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 50
http_threads = 4
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = flood http bobbear.co.uk
ufreq = 5
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= SomeCustomInjectedHeader:injected_by_wvs
attack_mode = 0
max_sessions = 30
http_freq = 100
http_threads = 3
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = wait
ufreq = 5
botid = xMYHOST1_347EBCFB
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 10
http_threads = 2000
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = stop
ufreq = 3
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 30
spoof_ip= 1
attack_mode = 0
max_sessions = 30
http_freq = 20
http_threads = 5
tcpudp_freq = 60
udp_size = 1000
tcp_size = 2000
cmd = stop
ufreq = 15
botid = (not set)
```

```
icmp_freq = 10
icmp_size = 2000
syn_freq = 10
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 100
http_threads = 3
tcpudp_freq = 20
udp_size = 1000
tcp_size = 2000
cmd = stop
ufreq = 10
botid = (not set)
```

```
icmp_freq = 40
icmp_size = 2000
syn_freq = 2000
spoof_ip= 0
attack_mode = 0
max_sessions = 30
http_freq = 20
http_threads = 1500
tcpudp_freq = 4000
udp_size = 4100
tcp_size = 4000
cmd = flood http
ufreq = 1
botid = xMYHOST1_347EBCFB
```

Responses to mule recruitment

- Currently favorable conditions
  - Lack of mass acceptance of virtual currency, allowing good old fashioned “follow the money” techniques
  - Active money mules/victims are the best source of raw intelligence
  - Victims in ongoing relationships must be “hijacked”
  - Building and utilizing an inventory of bank accounts, and phone numbers operated by LE in order to infiltrate and then expose their bank accounts
  - Easy to monitor DNS infrastructure allowing real-time discovery of domains that haven’t even been spamvetised yet

Final words

- The security industry shouldn't be like the health industry => treating the decease is far more profitable than curing it
- OSINT (open source intelligence) is so powerful when combined with historical OSINT (databases) that you don't need to become a cybercriminal in order to catch a cybercriminal
- Perfect conditions to hit the ecosystem at all fronts, due to their wrongly perceived invincibility